Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Фізико-технічний інститут

Криптографія Лабораторна робота №3 (варіант 6) Криптоаналіз афінної біграмної підстановки

Виконали: студентки 3 курсу ФТІ групи ФБ-93 Шрейдер Марія Жембровська Олена

> Перевірила: Селюх П.В.

Мета роботи

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Порядок виконання роботи

- 0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
- **1.** Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.
- 2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).
- **3.** Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв'язання системи (1).
- **4.** Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не ϵ змістовним текстом російською мовою, відкинути цього кандидата.
- 5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Хід роботи

В ході роботи ми йшли за пунктами з «порядку виконання роботи».

Помітили, що в алфавіті, яким шифрувався тест були переставлені місцями букви «ы» та «ь».

Найчастіші біграми шифртексту

Розпізнавач російської мови

Був обраний ентропійний критерій відбору змістовного тексту.

Для розшифрованих текстів по кожному зі знайдених ключів рахується ентропія тексту без пробілів та порівнюється зі значеннями, які були знайдені в першій лабораторній. Це приблизно від 4.4 до 4.5.

Повертається ключ, за яким ентропія розшифрованого тексту входить в даний проміжок.

Зашифрований текст

ывлеюгзебщпещхщуйэвиывиюфгувхцубхшыюнюжлепэшфмиьхдощбуднзегдщебоцвшуюгьпцвэ щувкмзеиэбчиюндхщюасдбмонхегщгдэщжезьщемвощфысьмайыегыйяййыэшжеаекидщщеюжгь деьцонгочвнюимыжымудеьбюгьщесфвшвоюзйэящкщьюгочвнюлмшужеейцурпцвдэяхщамьдеу эвющэвдиайятвепцвчвлеюйщецыаешвэеяикгехщаэациэибвкмрйжуажййдекущтепэшфмздсу пьвоцьяй дижури в при в юэзопюзкнэщегбдсефвьхбжщенюцатщввэиегтеаехохтюйлдицзьхдщшшюяьзщюоцвлеюосдлу злзащавызйферддьйомюиаыьепжмнюбжщцаещэзойтзэвзвщупмюжьощшаощвыжееююззьдеаей ющдоездюйбигьвиюэколищхмоихсшфеэмлеотзомщивхцывбжхебахиэьщхизашжеттфележебд фюфпнюфмшуиэжяппшдгдшесдиживхеюцхеяднвжееютбзййысддемилпмюзахшнюлллоюэпподй шяюь хщужиуцтабззлзьйопнбоящпи видовних дбднвншлврпшилмиь адшахушайы эффтппмю цдсззезщадць цихжшуфгбиэихеныжпбоцднесдегмаущйыктгдыйктййнвмоктздгидатаомтщл вхеийрдимяцшуьюывмтшзюашнэьгоэавюрдвджгмпиээщеиэивдодзехатщйыэшззшзунзщхеюи зчсдэайэхенвжьфжисхгчилвжмвиртдэнишуртцюиэннедчйдещоридивюбжлотвдюлофехшыдд етеодаьйояхрдбмлпнднелеыщхдощуцщазнибыутвднтащебацэзьгордфесьаещзкнсднюятьд аахмчвюцхеиовющежемпзькюжямюгьщцсбвдсчепзлепэшбмтвгоэвубюзмвппцинэзьэщтапуи эпхлеоенщнщрдэщлабмхтфуиюййаещэдэвлюцрпбжэщыдидсдщохилпийшгмищцвюбйощйапедм лесгцать чщбуэь гйцами эавдкю яцрорпбдкь йомь ще аохдяю чвей чвэ ухвь хэерю чежюш зю ахмр пяйзхфйдыжецэзчящктмоодььепюйяйрйощоюцдиеиатщхщнеэмьхгьощщооиьвдгивыжшухе ияйхмлпияюцмахщмайвкмшуовывбочвгййобуиэывзджююцгйбасдйэвюэасуяхуцбущуфтлпэь вмхшоеяхрпдюцибофебаитвлпхлпэьуеюююэлпбийэлпбинюфугьвоцвхестюцгдтэфйнеэатщщ авытдщааошумюжячеаееоодзтлояййысьюцсьмашайыьхлеяюсбфеюоэщуйзлепрдюйкизолюуц обуйюгктнвэииюдэяхщагююцхенедефепэлпсаийкиящбушзшзунтахаьыхдрпдэьщчижеьюхиб унюзьдесьюцаетщфеюайвкмжгеэзчхаздхенехднвящжесьвчаеяютвючсьцукммюфпэьхцхене ещжпмюфгцвцвзщящдыээжежуйэфгэзюайычщоднвкгшвиьвчлпэьяьхэжмьхиьбщйыфпжягьмат щаефмлесгцадьтцэьакгдйпгцэьдемимоэщчртщгдьцэьшщузмюнпамвикнсшувлонвиюовкмле бпчвмвзьжемвшзгдяиампнлоппбообхдвыхщнвшуялнюгьэабуохобхдзечадыегжеыщхдктеаю аирюунедмщуудвайыэанвфупдэмчвмьщелеяймоюааачвэуопэьжеюэюааееыпхщаэаяхзснгые тепюхиэь аелецюктпм эшршеь бюекгдь втщшдчи убждгдхеь цкнвю и эв днв фузчшшдет адшим жйц умюэщчйощйаэмтщвдеьйомюхебавахивлфеионвздоюубтесаыдхщнвшуцуюэрдцзщхмвлоцущц шайюшдрддебочищукмжйпиуцфйжпщцоеидфгшйощемлмжгвдфвюаюообюаюьймвшжеэуяххарин дщшэщгщчикгялнювамжфуощпйццмюегнещеегбдфюфпюйбпгьфпжяиэцвтбнещеегбмлещщзеяй ьддь яецыфгсцфжтбшв яцвиощиалещщнв бчрйхаюию чпммьш г я ошулобжфгфиыж пптбшвиьййраы ьнщеаощяэшулопдицщццаявяцбуиьэщхдвыбщпееыаебухтвдсдощийыщцыэщзщцймилмлежщощ расгиацэиюшшыйзащеоюиьцвитшэлебджювшшжиужиубяэшулопдхомццвяйощвыявжявщэаадо щыщтщкщфйыьжеуцщуыднвлеьэяхщабммоппмвппдюлмледшяйдужижиженввиищятпнзетечютд юйбпгь чизднвепфйзщиа кунэшщфпызяйть хиэиианв зшущиор пбдпюцижефв чвйэгцлпнющецыа еямтщтаэаощськимочиэилпбоодэаьдааощчвощоющдийрднпцвдщнюиадежпиэвиьхсшрдехщу иэтфппфакподимприженирокинодехпшоеранары азынары жайын ьчвдодэйайыжевыоененезаиаразевыбвжйцулмлепеяшдерйхаюииэяхщагютврюфпэшиацаыв вюсюлою эуцвшэщйы аегюфпгь пднеи зящсджпних езефюфпящ чвэвь хлимь дшоюь хиьрйрарежюг ьщелекщтьээмофзнэцвсдмааеюиэисьмюцвэиубэфгщдещечйшвюзкоусжээщтеяииюфггщкеею ччэацапесь зецюмозь хцоуоеуюмодшяййых етеуиэижецээчтэгчяййыбозэгчяййымааейшгюд пюйбпгьищщхйэзьлвепцвсдчйыутвывяцбехдыиьхзавдсщяобамщсдэанелезатэфйфщиээщне жетщгдидчвряоеуюжйжпннтвшивлугцхлехщтапэсбеелеяоодгджюубвюцдеюччщупнлмлеяеш айымалимьящфгмючехйуышзкоусбщмазщбиьхзазьйысьзьюауйжекюжмтщкдцьщхйэашцааюцв мабзнэщежееюсюбжовщцэапейцщцвюлозьйычвййзаятдпэшьхлеяюсбеужищеегдьдэбоодфее аоененетщкервтвэитэщанезчудйожецэзчкмючсджээлрдяюнюиюээмюсетпыжтащенепхсшыщ ьвчвнюлоиэяцсбэапепещдйогдыйхедетамайвднвюдэяхщавомоодбпртгьоецуппиачпковфн дхщоедесшсдкюэьдэяцсдцааюцвэщфепэюцзасеяинэшзчуртэщсззееысдкюмвежцищемарцзл

цвпепемайыщпзьуасьцвэиюэяхщавоцэлеююфпрдеыэвчвтааеувэетеьджюсббамщиаиьмахен щщавысьщияцодчэтдбщпенегдеаиююуэзлвиюэзлпмотвяьреэщдепвлпзшшаощсуяхсуяхлпви дшхщпелееецацабацыешэщеггдюпшшмүкнвюутючшабщошшшэшжлзьдшфглоиэюаэьубяшбммыш гжюуббуиьппбжхееэщуьхамьхфйсщощвыятжмючктюцощщпвлхешекюиэзосднефепэчщущхдиж ппчиртлпчврянюбоодщэзопсеьаохтгднщхекудээиэибацыещкибохтгдййаююэяхщаяэяхщав онвздадяйтьреошиынщмаонгоюзщатаььта эазехдвьнинв эь дюртюцгсдее эюцгишүчнүлнлм жмящнюпхмьшияцдеыуппамрпзьроадздыщчврялежпсбамгдещнвсбэаэщьэяхщаеадежпиээщщ ьюцмюепаелешткитвяцдееюдпэьдюиюложьвиибпейцамиьоецуппбозацыжервщцжиртлпцацы тдоехдсвщцюзмвусщекуяцфгкмрпцвсдчйбщцщлоцвкгвюфттщнгкмжгпййождгдфгнхрйжщиак вбжхебуктюаоюцдзшшгюйбпгьбпбюфпбвмьщелеяйэщшднесдроюэппамбжронвжешать эзребц июывэцчврятазшрдюйкизоажхенежетщттххдэтахшшисьцвэиюэяхщалттвящуэбчиюндамтщж пунлпэшшвчвйэрпуюиьрйещйыэшдеюйбазеашлльюусзочвцаделекюцииайгшацвэшвдсдтщео рпиьчврясдщелечпбопнххлпфмшуиэщщсдлоиэледещохиболпжйсднегужиоаэвбжронвпйцвг щнюаеегыюфпждвпщюиьаепзкнбатахщьпсефггдяилмепэшэвчвадздююубиьмюмтчеодеычмдэ лпепэьйыямвиртюцсшсднвлптвэиубшштиубзчшгыьгйцаоиэивюрдрячиртлпщещьмоодяюзьж гхюйэяхщабмчвлеааатюцгсхеэщшднесдюфывепнюсьлоздшшианвшузлмюхебуэьрймшшатьтц ьеэуллмюзэгцлинюшвчвиьрйещеьбюбжщенюиьмахенщтьаобчйэылщхрдшгматжщешгмааеюцж ьтджювитщразервяцсехдйнощзацыбддебщпезмйэтвощжестюцгдиавоцвмюцвэулллотвнюжн мющхлеуииь таэазехдющдетаэадужиубхошунхрдощнвшардздхылофмгдмащавыцюэздщощоея дь эхвдюэзмочпцвлпиь гоощнвпйсь шузохефпызяйть рехджоод эввифйяд шаждгдфгг щ нерйюг лофцчвтщхдвыпелебдеыаеьйнщыщхдгдбмгдхдбщььзецюьхнэсфибнвиювичврянвзшрйвдздж юлмгчхтзбчишшюаюьтайгшаошюсэшййшоэшещяйгдтидшвоюзйэхесдегжщюаыьзекжгь щенюэь щифижштыыь жеуцюаюь та эах шүнө эвь хэеэ шүхдүгиндид вою эйэс двүшүгинлит шжпежүддеж гүнт во вднвюяхмощуепнюдещечйшвчвьхзанэудеьщйжпннтвшиэихещщеьаожецэзчкмопияжмрплобч ццыцвэшявхжпдидьдмаеылочводэжгьюйбауэяхщавочвножйядтпктаевшээмиолоылмьмоодпз агючвяцсехдзюэизеэщощвыамьхфйсщощфйзщшнюучаущюимьюжфучугьоддпэьовлмяхусидгщ кухтхеажщедещию аугша зевыт пктепиь схчвиою зопщувю ыв яьчщдецуыь бщихй эунищиж фтзел ммьщебджюсбюанвшубюфгеэяхщаыйцачюэирпмюамлпияцднеунощбпвзвимождгдяйдвмюьщег фгыюфпсесакумюфгоажгшьвияцжпмохенюятздэаьпзьхегехшыйяйдужибочвэухвэсюаяйбац ыещзщэабвюатайывдсуыжывдюиэмошушйиадечюмюзэциуцнщхекудэяцепзьхестюцсшэщаеио вифйлхнэлвижппикщежесьмюкмщджгмяппсбхщжвччнюшияцюужгщдеьжечмзьмюййнежетщщех дйанюэьюэлвиаэабнппяцнвжегдпмзобднердздшамйдвеавэнщещамхвусеьыьрйчайыгдчиэи жпунудщехехдьжыввмиькдбовшвыэьаееадебпээкоудкюдэяхщаеапехдизопбжщещечирттвд юлмлеоелжличвййщигдидййтельиюдохжящэаюйбатьцчгдкьвдюжвюубщизьсюцвбжщефебали мьтесьюцсуяхубвдыюэенвздажщеощшшежэудеьоезелаллжмадбщяиэиюайгкукоудеьээя хщабмшузьмасллотвьщдецуьхлпйтаияцгпэзбоцвещяйсдкюцвюзаихевджюсбеавэнщшвяцзщ цюфпбуйэрпхаьллотвюшдеэщбачмжмвддыллкмбжбшжпежепиьаэгцуджэяхщагюфтианжщеэвн юэехеяецыойидкмхшоекуяцдэхеажщещещхиьнйююфпьхрдяднючвкмшууеошйыунзебвчвййнв сдчхрдщеэаяюубсдкюцвцэзьовывхшфеьэяхщащщбмйэбщкижмюфпмлпвоубкщжещехеэфлошус деьбюдэчврпшинююцхеиилмйэзлзайыяецыхесдийрддшлльюуссдэахдоехеаеяюкмтщрдкюхт ыжюцядэащдба

Ключ

(441, 310)

Розшифрований текст

утробылотихоегородокутанный тьмой мирнонежился впостели пришлолетои ветербыллетний теплоедых аниемиранес пешное иленивоестои тлишь встать высунуть сявокош коитот час

поймешьвотонаначинаетсянастоящаясвободаижизньвотонопервоеутролетадугласспол дингдвенадцатилетотродутолькочтооткрылглазаикаквтеплуюречкупогрузилсявпредр ассветнуюбезмятежность онлежалвсводчатой комнатке начетвертом этажевов семгороде небылобашнивышеиоттогочтоонпарилтаквысоковвоздухевместесиюньскимветромвнемр ождаласьчудодейственнаясилапоночамкогдавязыдубыикленысливалисьводнобеспокой ноеморедугласокидывалеговзглядомпронзавшимтьмуточномаякисегоднявотздоровоше пнулонвпередицелоелетонесчетноемножестводнейчутьнеполкалендаряонужевиделсеб ямногорукимкакбожествошиваизкнижкипропутешествиятолькопоспевайрватьещезелен ые яблокиперсикичерные какночь сливые гоневытащить излесуизкустовизречки акакприя тнобудетпомерэнуть забравшись взаиндевелый ледниккак веселожарить сявбабушкиной к ухнезаодностысячьюцыплятапоказаделоразвнеделюемупозволялиночеватьневдомикеп ососедствугдеспалиегородителиимладшийбратишкатомаздесьвдедовскойбашнеонвзбе галпотемнойвинтовойлестниценасамый верхиложился спать в этойобителику десника сре дигромовивидений аспозаранку когда дажемолочнике щене звякалбутылкамина улицахонп росыпалсяиприступалкзаветномуволшебствустоявтемнотеуоткрытогоокнаоннабралпо лнуюгрудьвоздухаиизовсехсилдунулуличныефонаримигомпогаслиточносвечкиначерно мименинномпирогедугласдунулещеиещеивнебеначалигаснуть звездыдугласулыбнулсят кнулпальцемтамитамтеперьтутивоттутвпредутреннемтуманеодинзадругимпрорезалис ьпрямоугольникивдомахзажигалисьогнидалекодалеконарассветнойземлевдругозарил асьцелаявереницаоконвсемзевнутьвсемвставатьогромный домвнизуожил дедушкавыним айзубыизстаканадугласнемногоподождалбабушкаипрабабушкажарьтеоладьисквознякп ронесповсемкоридорамтеплыйдухжареноготестаивовсехкомнатахвстрепенулисьмного численные теткидя дь ядвоюродные брать яисе стрычто сехались сюда погостить улица стар иковпросыпайсямиссэленлумисполковникфрилеймиссисбентлипокашляйтевстаньтепро глотитесвоитаблеткипошевеливайтесьмистерджонасзапрягайтелошадывыводитеизсар аяфургонпораехать застарьемпотусторону оврага открылисвои драконь игла заугрюмые о собнякискоровнизупоявятсянаэлектрическойзеленоймашинедвестарухиипокатятпоут реннимулицамприветственномахаякаждойвстречнойсобакемистертридденбегитевтрам вайноедепоивскорепоузкимрусламмощеныхулицпоплыветтрамвайрассыпаявокругжарки есиниеискрыджонхафчарливудменвыготовышепнулдугласулицедетейготовыспросилону бейсбольныхмячейчтомоклинаросистыхлужайкахупустыхверевочныхкачелейчтоскучая свисалисдеревьевмампаптомпроснитесьтихонькопрозвенелибудильникигулкопробили часыназданиисудаточносеть заброшенна яегорукой сдеревьев взметнулись птицыи запел идирижируясвоиморкестромдугласповелительнопротянулрукуквостокуивзошлосолнце дугласскрестилрукинагрудииулыбнулсякакнастоящийволшебниквоттотодумалонтольк ояприказаливсеповскакаливсезабегалиотличноебудетлетоионнапоследокогляделгор одищелкнулемупальцамираспахнулисьдверидомовлюдивышлинаулицулетотысячадевять сотдвадцатьвосьмогогоданачалосьвтоутропроходяполужайкедугласнаткнулсянапаут инуневидимаянить коснулась еголбаинеслышнолопнулаиотэтогопустячногослучая онна сторожилсядень будетнетакой какв сенетакой еще и потомучтобывают дни сотканные и зодн ихзапаховсловновесьмирможновтянуть носомкаквоздухвдохнуть ивыдохнуть такобясня лдугласуиегодесятилетнемубратутомуотецкогдавезихвмашинезагородавдругиедниго ворилещеотецможноуслышать каждый громикаждый шорохвселенной иныеднихорошопробов атьнавкусаиныенаощупьабываютитакиекогдаесть всесразувотнапримерсегодняпахнет такбудтоводнуночьтамзахолмаминевестьоткудавзялсяогромныйфруктовыйсадивседос амогогоризонтатакиблагоухаетввоздухепахнетдождемнонанебениоблачкатогоигляди ктотоневедомый захохочетвлесунопокатамтишина дугласвов сегла засмотрелна плывущи емимополянетнисадомнепахнетнидождемдаиоткудабыразнияблоньнетнитучиктотаммож етхохотать влесуавсетакидугласв здрогнулдень этоткакой тоособенный машина останов иласьвсамомсердцетихоголесаануребятанебаловатьсяониподталкивалидругдругалок тямихорошопапамальчикивылезлиизмашинызахватилисиниежестяныеведраисойдяспуст ыннойпроселочнойдорогипогрузилисьвзапахиземливлажнойотнедавнегодождяищитепч елсказалотецонивсегдавьютсявозлевиноградакакмальчишкивозлекухнидугласдуглас встрепенулсяопятьвитаешьвоблакахсказалотецспустисьназемлюпойдемснамихорошоп

апаионигуськомпобрелиполесувпередиотецрослыйиплечистый занимдугласапоследним семенилкоротышкатомподнялисьнаневысокийхолмипосмотреливдальвонтамуказалпаль цемотецтамобитаютогромныеполетнемутихиеветрыинезримыеплывутвзеленыхглубинах точнопризрачные китыдугласглянультусторонуничегоне увиделипочувствовалсе бяобм анутымотецкакидедушкавечноговоритзагадкамииивсетакидугласзатаилдыханиеиприс лушалсячтотодолжнослучитьсяподумалоняужзнаюавотпапоротникназываетсявенеринв олосотецнеторопливошагалвпередсинееведропозвякивалоунеговрукеаэточувствуете ионковырнулземлюноскомбашмакамиллионылеткопилсяэтотперегнойосеньзаосеньюпад алилисть япоказемлянесталатакоймя гкойухтыя ступаю какиндеецска залтом совсем несл ышнодугласпотрогалземлюноничегонеощутилонвсевремянастороженноприслушивалсям ыокруженыдумалончтотослучитсяночтооностановилсявыходижегдетытамчтотытакоемы сленнокричалонтомиотецшлидальшепотихойподатливойземленасветенеткружеватоньш енегромкосказалотеципоказалрукойвверхгделиствадеревьеввплеталасьвнебоилимож етбыть небовплеталось влиствувсеравно улыбнулся отецв сеэтокружева зеленые иголубы евсмотритесь хорошень коиувидителесплететих словногу дящий станокотецстоя луверен нопохозяйскиирассказывалимвсякуювсячинулегкоисвободноневыбираясловчастоонис амсмеялсясвоимрассказамиотэтогоонитеклиещесвободнеехорошоприслучаепослушать тишинуговорилонпотомучтотогдаудаетсяуслышатькакноситсяввоздухепыльцаполевых цветовавоздухтакигудитпчеламидадатакигудитавотслышитетамзадеревьямиводопадо мльетсяптичьещебетаньевотсейчасдумалдугласвотоноужеблизкоаяещеневижусовсемб лизкорядомдикийвиноградсказалотецнамповезлосмотритеканенадоахнулпросебядугл аснотомиотецнаклонилисьипогрузилирукившуршашийкустчарырассеялисьтопугающееи грозноечтоподкрадывалосьблизилосьготовобылоринутьсяипотрястиегодущуисчезлоо пустошенный растерянный дугласупална коленипальцые гоушлиглубоков зеленую теньивы нырнулиобагренные алым соком словноон в эре заллесножом и сунулруки в открытуюранумал ьчикизавтракатыведрачутынедоверхунаполненыдикимвиноградомилеснойземляникойв округгудятпчелыэтововсенепчелыацелыймиртихонькомурлычетсвоюпесенкуговоритот ецаонисидятназамшеломстволеупавшегодереважуютсандвичиипытаютсяслушатьлескак слушаетонотецчутьпосмеиваясьискосапоглядываетнадугласахотелбылочтотосказать нопромолчалоткусилещекусоксандвичаизадумалсяхлебсветчинойвлесунеточтодомавк уссовсемдругойверноостреечтолимятойотдаетсмолойаужаппетиткакразыгрываетсяду гласпересталжевать ипотрогаля зыкомхлебиветчинунетнетобыкновенный сандвичтомки внулпродолжаяжеватьяпонимаюпапведьужепочтислучилосьдумаетдугласнезнаючтоэто ноонобольшущеепрямогромадноечтотоегоспугнулогдежеонотеперьопятьушловтоткуст нетгдетозамнойнетнетздесьтутрядомдугласисподтишкапощупалсвойживотоноещеверн етсянадотольконемножкоподождать больноне будет яуж знаюне за темоноком непридетноз ачемжезачема

Висновки: в ході лабораторної роботи дослідили та реалізували метод розшифрування шифру афінної підстановки біграм. А також дізналися про критерії відбору змістовних текстів і реалізували один з них.